Chapter 30 - Physical Security Policies

3001 Purpose

The Manual of Security Policies and Procedures ("Security Manual") implements the policies and procedures that govern the management and administration of the personnel, information, and physical security programs of the Department of Commerce. Section IV of the Security Manual prescribes the policies, procedures, and standards that govern the implementation of physical security measures designed to protect personnel, facilities, property, and information in the Department of Commerce. The manual also specifies the minimum physical security standards for the Department of Commerce.

3002 Application

A. The physical security policies and procedures described in the manual apply to all Department of Commerce operating units, offices, facilities, employees, contractors and associates, and others who have access to or use departmental facilities and assets. Provisions in this section take precedence over physical security policies of any bureau, operating units, or other offices in the Department; however, nothing in these regulations shall be construed as contrary to the provisions of any statute or Federal regulation. In the event of conflict, specific statutory provisions shall apply.

B. The senior official or manager of each operating unit, office, or facility in the Department is responsible for the safety and security of his or her personnel, property, and information. Managers have certain specific security responsibilities that are described in the manual. In addition, each employee is responsible for adhering to the security requirements prescribed in the manual. Employees or other personnel associated with the Department shall report any incident or condition contrary to these requirements to their security contact, servicing security officer, or the Office of Security.

C. Requests for exemptions from the provisions of the physical security requirements may be made to the Office of the Director of Security to meet unusual situations peculiar to specific organizations. A request for an exception must be made in writing and must set forth the justification and proposed alternate procedures for safeguarding or affording equivalent protection for the persons, property, or facilities involved.

D. Failure to comply with the Department's physical security policies, regulations, or procedures may result in administrative or criminal sanctions to include withdrawal of security clearance and disciplinary action that could range from counseling to removal from Federal service. Violations of

a criminal statute shall be reported to the Office of Inspector General for possible referral to the Department of Justice.

3003 Physical Security Policies

A. To ensure the protection of departmental personnel and assets, physical security programs shall be established and implemented in each operating unit based on the minimum standards set forth in the manual and other appropriate laws, regulations, and national codes for the protection of life and property. These programs shall be administered and monitored continually to ensure their integrity. All security standards will be met in new facilities whether constructed or acquired by purchase or lease. Every attempt will be made to acquire sites or new facilities that meet physical security standards. In the event that one or more standards are not met for a specific building, requests for exceptions may be requested by the departmental organization to the Director of Security.

B. Operating units on Federal property under the control of the General Services Administration and having a security delegation of authority from GSA must provide for the security and protection of personnel and assets within the property. Based on the Presidential Policy Memorandum, "Upgrading Security at Federal Facilities," the head of the operating unit shall upgrade and maintain security in their owned or leased facilities to the minimum standards specified in the Department of Justice study, "Vulnerability Assessment of Federal Facilities," June 28, 1995.

C. The facility manager, in conjunction with the servicing security officer, shall conduct a survey of each facility under his/her jurisdiction to determine the type and extent of security controls necessary for each facility or area. Physical security surveys shall include a security evaluation (risk assessment) that addresses the criticality of operations, the vulnerability of the facility or area, and the probability of loss or damage to facilities or property and danger to personnel. The servicing security officer shall assist the facility manager in developing a security plan for addressing any recommendations resulting from the surveys, inspections, or self-administered checklists. All recommendations shall be coordinated with the Office of Security.

D. The extent of exterior and interior controls will be determined by considering the monetary value and mission criticality of the items or areas to be protected, the vulnerability of the facility, and the cost of the controls. Normally, the cost of security controls should not exceed the value of the item or area to be protected.

E. A restricted area requires special restrictions or controls to safeguard property or material. Admittance to a restricted area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area. Personnel without an appropriate security clearance must be escorted in a restricted area where classified material is produced, processed, or stored by

personnel assigned to the area. When uncleared personnel are present in a restricted area, classified information must be protected from observation, disclosure, or removal. The security contact or office manager is authorized to designate an area as a restricted area after adequate security measures are in place.

F. Each employee, contractor, or associate of the Department is required to possess and carry a form of identification while in duty status, and will be subject to local restrictions prescribed by the facility manager. All personnel in a facility identified as Level IV or V shall display a photo ID on their person above the waist at all times. The displaying of a photo ID in other facilities is recommended.

G. Identification (ID) forms shall be restricted to those critical to the accomplishment of the Department's missions. Special forms of identification for unique purposes or special facilities require justification. An example is the Census Bureau's enumerator ID for special censuses. Any proposal for a new form of identification shall be submitted in writing with a detailed justification through the servicing security officer to the Office of Security for approval.

H. Each person within a departmental facility, regardless of position, shall be subject to challenge by another departmental employee, the servicing guard force, the security contact, the servicing security officer, or any law enforcement officer, and shall display appropriate identification when challenged. Failure to do so may result in removal from the facility or other administrative action.

I. Department of Commerce facilities house a wide variety of functions and activities that are performed by Federal Government employees, departmental associates, official visitors, foreign nationals, and the general public. Access to departmental facilities during and after business hours shall be controlled as specified in local security procedures. Policies and procedures for access to local departmental facilities shall be established by the ranking unit official or senior facility manager and shall be in compliance with the policies and minimum standards set forth in the manual. Decisions on admittance policy shall take into consideration the sensitivity of the facility, the criticality of the operations, existing access controls, including guard forces and their response capability, alarm systems, and the investigative process completed on the persons who will have access.

J. Department of Commerce facilities are normally open to the public for official business during regular business hours; however, access is normally restricted after business hours to protect departmental assets. Certain facilities may not be open to the public even during normal business hours due to local restrictions. Special access controls must be observed in these facilities. Security hours are those hours a facility is closed to the general public where access must be limited to individuals essential to the official business of the Department. The facility manager shall institute access controls for Department of Commerce facilities during security hours.

K. Non-employees such as visitors and family members may be admitted to facilities subject to local procedures developed by the facility manager and the servicing security officer provided such visits do not disrupt the normal business of employees. Facility managers or servicing security officers may utilize a registration form or other written record to obtain an employee's acknowledgment of this responsibility. Areas may be closed to public access when circumstances require action to ensure the orderly conduct of government business. The decision to close public areas shall be made under GSA Federal Property Management Regulations or local requirements in consultation with appropriate security officials.

L. When identification forms are required for admittance to departmental facilities, employees or maintenance and contractor personnel shall display an authorized form of identification at all times. Some departmental facilities may be closed to employees, contractors, and other persons as special circumstances warrant. During such special restrictions, supervisors may need to provide lists of essential persons to the facility manager or security officials to arrange for authorization to enter the facility. A completed CD-165, Admittance to Department of Commerce Installations During Security Hours, or a memorandum may be used for this purpose. Union representatives will normally be granted access to their union offices and files if conditions allow.

M. The ultimate decision to control access to a facility rests with the facility official who shall consult with the servicing security officer. All access control procedures shall be established in accordance with the standards prescribed in the Department of Justice Standards for Federal Facilities. If necessary, the facility manager may strengthen the access control procedures in the manual. On the other hand, to accommodate unusual operations, facilities, or circumstances, local officials may prescribe less restrictive admittance procedures provided they are within the guidelines established by the Department of Justice Vulnerability Assessment of Federal Facilities.

N. Personnel should immediately report missing office keys to the issuing office. The servicing security officer should conduct a security evaluation to determine if it is necessary to re-key the office. Security contacts, facility managers, or other issuing officials should institute a 10-day waiting period before the replacement of lost keys. The waiting period will allow time for a lost key to be found before expending the time and expense of issuing a replacement.

O. All positions in the Department encumbered as police officers or law enforcement officers (LEO) and required to carry firearms in the line of duty will be designated High Risk at a minimum and will be processed in accordance with Chapter 10, Position Sensitivity Designation, of the manual. Police officers or LEO personnel occupying a position that requires access to classified material will be designated Critical-Sensitive. Special departmental investigative processing is required for armed guards, and certain other precautionary measures must be taken by selecting facility and security officials to reduce the possibilities of mishaps involving firearms.

P. Security containers utilized for the storage of classified information shall be controlled by the security contact in an operating unit in consultation with the servicing security officer. When possible, records of security container use shall be recorded in the Department's electronic database system, Security Information Management System (SIMS). If an operating unit or other departmental office does not have access to the system, appropriate records, electronic or written, shall be maintained by the servicing security officer or the security contact to ensure the accountability of security containers. The Classified Control Point (CCP) in each operating unit is responsible for recording information into the SIMS, their own electronic system, or a written record, and for assisting the security contact in maintaining such a record.

Q. Prior to procuring new storage containers, managers should make an effort to retire, return, declassify, or destroy unneeded classified records, files, or materials to make storage space or containers available. Managers shall also check with property management personnel to determine if surplus containers are available prior to purchase of new containers.

R. A large number of filing cabinets with security lock-bars and padlocks in the Department have been conditionally approved for classified storage up to the Secret level. However, lock-bar filing cabinets are easily compromised and do not provide adequate protection for classified information. Therefore, these containers must be phased out of use by October 1, 2012. Until October 1, 2012, material up to the Secret level may be stored only if the equipment is already in use. These cabinets must be systematically phased out and be replaced with newer GSA-approved security containers.

S. Volumes of valuable and critical property pass through shipping and receiving areas daily. Managers often create areas for the storage of new or used equipment waiting for distribution. If not properly protected, the areas become vulnerable to theft and misappropriation of the stored equipment. Storage areas should be located away from shipping and receiving areas and facility entry and exit points to make the unauthorized removal of stored items more difficult.

T. Procedures shall be established for the control of incoming property, and shipments shall be checked for signs of pilferage or damage. A careful inventory of incoming shipments shall be conducted to assure that all items on the bill of lading or other manifests is received. Delivery records should be checked against requisitions and purchase orders. Only designated personnel with completed background investigations who have been determined to be trustworthy shall be authorized to accept or sign for deliveries. Damaged merchandise should be separated and secured until disposition can be made.

U. GSA regulations require that all property leaving Federal facilities be accompanied by proof of authorized possession or ownership. The form presently in use in the Department for this purpose is the Optional Form 7, Property Pass.

V. Automated information systems and facilities require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems, facilities, and tape storage areas shall be protected from theft, alteration, damage by fire, dust, water, power loss and other contaminants, and unauthorized disruption of operation. The extent of physical security measures needed is determined by the results of a risk assessment and/or a physical security survey.

W. At a minimum, computer facilities should be designated as a controlled area. A major computer facility shall be designated as a restricted area in which access into the facility is limited to personnel who are assigned there or who are authorized access by the facility manager.